UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. DENNIS COLLINS, ET AL., Defendants.	Case No.: CR 11-00471 DLJ (PSG) **AMENDED ORDER DENYING PLAINTIFF'S MOTION FOR RECONSIDERATION** **(Re: Docket No. 284)**

Among other things, the March 16, 2012 order of this court gave the government 30 days to undertake a reasonable effort to return data to defendants.[1] The data at issue fell outside the scope of the 27 warrants by which over 100 of the defendants' computers and other digital devices (including storage media) were seized.[2] After securing leave from the court,[3] the government now seeks reconsideration of the court's return order.[4]

[1] *See* Docket No. 237 at 12. At the government's request, this deadline was extended. *See* Docket No. 249.

[2] *See id.*

[3] *See* Docket No. 267.

[4] *See* Docket No. 284.

In its March 16 order, the court already outlined *Tamura, CDT* and other pertinent Ninth Circuit precedent, and will not do so again here. The grounds for the government's request are as follows: (1) identifying non-targeted data might be difficult; (2) certain non-targeted data might be useful in understanding data that is clearly targeted; and (3) disaggregating non-targeted from targeted data might be unduly burdensome and expensive; (4) allowing only the defendants to keep a complete copy of the seized data might deprive the government the ability to challenge exculpatory non-targeted data and thus would be unfair. As evidentiary support, the government offers a declaration from Alan Lee, Deputy Lab Director and Operations Manager for the Silicon Valley Regional Computer Forensic Laboratory.

The court is not persuaded. Mr. Lee's declaration confirms that almost a year and a half after presenting the warrants, the government has yet to take any meaningful steps to isolate non-targeted from targeted data. Each of the grounds offered by the government either was presented or could have been presented months ago, before the court issued its March 16 ruling. On this procedural basis alone, the government's request is deficient.

More fundamentally, the government's argument proves too much. If separating non-targeted data from targeted data and devices lawfully retained as criminal instrumentalities is too hard here, it presumably is too hard everywhere. In what case where a storage device is seized lawfully could a defendant or other subject of a search warrant ever secure return of data that the government had no right to take? Just about every storage device can be searched more easily with automated scripts than manually.[5] Just about every storage device has non-targeted data that might prove useful to understanding the data that was targeted.[6] Just about every storage device has

[5] *See* Lee Decl. ¶¶ 5-8.

[6] *See* Lee Decl. ¶ 15.

deleted files in unallocated space.[7] If the government's argument were accepted here, so that it need not return even one bit of data that is clearly outside the scope of the warrant, the court thus would render a nullity the government's pledge in just about every search warrant application it files in this district that it will return data that it simply has no right to seize.[8]

The motion for reconsideration is DENIED.

IT IS SO ORDERED.

Dated: 8/8/2012

PAUL S. GREWAL
United States Magistrate Judge

[7] *See* Lee Decl. ¶ 14.

[8] *Cf. United States v. Metter*, No. 1:10-cr-00600-DLI, 2012 WL 1744251, at *9 (E.D.N.Y. May 17, 2012) ("The government seized 61 computer hard drives from Spongetech, four computer hard drives from Metter's home, and a snapshot of all of the activity that had occurred in Metter's personal email account. The government then promptly imaged the hard drives and returned them to their respective owners. Up to this point, there is nothing problematic with the manner in which the government executed the warrants. The point at which the government faltered is its delay in reviewing the imaged evidence to determine whether the evidence that the government seized and imaged fell within the scope of the categories of information sought in the search warrants"). Accepting the government's argument would also have the effect of shifting to the defendants the entire burden and cost of identifying targeted data to permit disclosure of any targeted data among the defendants. *Cf. id.*, at *9 ("Moreover, the government repeatedly asserted its intent to release indiscriminately the imaged evidence to *every* defendant, prior to conducting any review to determine if it contained evidence outside the scope of the warrants. The court agrees with Defendant that the release to the co-defendants of any and all seized electronic data without a predetermination of its privilege, nature or relevance to the charged criminal conduct only compounds the assault on his privacy concerns").